IN THE CLAIMS

Claims 1-10   (Cancelled)

11.   (Currently Amended) ~~A person authentication system according to Claim 1~~ A person authentication system for executing person authentication through comparing a template serving as user identification data which has already been acquired with sampling information input by a user, said person authentication system comprising:

a person identification authority for creating a person identification certificate storing the template;

an entity which executes person authentication for comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate; and

an entity which requests person authentication for requesting to said entity which executes person authentication for person authentication,

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider verifies a signature of said person identification authority written in the person identification certificate provided by said user device and transmits the result of verification to said user device, and

said user device decrypts, by using a private key of said user device, a key for encrypting and decrypting the template, the key that has been encrypted by using a public key of said user device and stored in the person identification certificate and provides the decrypted key to said service provider, with the sampling information input by a user, on condition that the signature is verified to have never been tampered with,

whereby said service provider that is said entity which executes person authentication decrypts, by using the key for encrypting and decrypting the

template, the template in the person identification certificate received from said user device, thereby performing person authentication.

Claims 12-24 (Cancelled)

25. (Currently Amended)~~A person authentication method according to Claim 15,~~ A person authentication method for executing person authentication through comparing a template serving as user identification data which has already been acquired with sampling information input by a user, said person authentication method comprising the steps of:

creating a person identification certificate storing the template by said person identification authority;

reading out a request for person authentication from said entity which executes person authentication; and

comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate in said entity which executes person authentication;

wherein said entity which requests person authentication is a user device, and said entity which executes person authentication is a service provider for providing service to said user device, and

said service provider verifies a signature of said person identification authority written in the person identification certificate provided by said user device and transmits the result of verification to said user device, and said user device decrypts, by using a private key of said user device, a key for encrypting and decrypting the template, the key that has been encrypted by using a public key of said user device and stored in the person identification certificate, and provides the decrypted key with the sampling information input by a user to said service provider, on condition that the signature is verified to have never been tampered with,

whereby said service provider that is said entity which executes person authentication decrypts, by using the key for encrypting and decrypting the template, the template in the person identification certificate received from said user device, thereby performing person authentication.

Claims 26-29 (Cancelled)